

# Constacyclic Codes over Finite Fields\*

Bocong Chen, Yun Fan, Liren Lin, Hongwei Liu

School of Mathematics and Statistics, Central China Normal University  
Wuhan, Hubei, 430079, China

## Abstract

An equivalence relation called isometry is introduced to classify constacyclic codes over a finite field; the polynomial generators of constacyclic codes of length  $\ell^t p^s$  are characterized, where  $p$  is the characteristic of the finite field and  $\ell$  is a prime different from  $p$ .

**Keywords:** finite field, constacyclic code, isometry, polynomial generator.

**2010 Mathematics Subject Classification:** 94B05; 94B15

## 1 Introduction

Constacyclic codes constitute a remarkable generalization of cyclic codes, hence form an important class of linear codes in the coding theory. And, constacyclic codes also have practical applications as they can be encoded with shift registers.

In [4], for any positive integer  $a$  and any odd integer  $n$ , Blackford used the discrete Fourier transform to show that  $\mathbf{Z}_4[X]/\langle X^{2^a n} + 1 \rangle$  is a principal ideal ring, where  $\mathbf{Z}_4$  denotes the residue ring of integers modulo 4, and to establish a concatenated structure of negacyclic codes of length  $2^a n$  over  $\mathbf{Z}_4$ . In [1] Abualrub and Oehmke classified the cyclic codes of length  $2^k$  over  $\mathbf{Z}_4$  by their generators. Generalizing the result of [1], Dougherty and Ling in [12] classified the cyclic codes of length  $2^k$  over the Galois ring  $\text{GR}(4, m)$ .

Let  $F_q$  be a finite field with  $q = p^m$  elements where  $p$  is a prime, and let  $\lambda \in F_q^*$  where  $F_q^*$  denotes the multiplicative group consisting of all non-zero elements of  $F_q$ . Any  $\lambda$ -constacyclic code  $C$  of length  $n$  over  $F_q$  is identified with an ideal of the quotient algebra  $F_q[X]/\langle X^n - \lambda \rangle$  where  $\langle X^n - \lambda \rangle$  denotes the ideal generated by  $X^n - \lambda$  of the polynomial algebra  $F_q[X]$ , hence  $C$  is generated by a factor polynomial of  $X^n - \lambda$ , called the *polynomial generator* of the  $\lambda$ -constacyclic code  $C$ . In order to obtain all  $\lambda$ -constacyclic codes of

---

\*E-Mail address: b.c.chen@yahoo.com.cn (B. C. Chen), yunfan02@yahoo.com.cn (Y. Fan), xiaomi1985516@126.com (L. R. Lin), h\_w.liu@yahoo.com.cn (H. Liu).

length  $n$  over  $F_q$ , we need to determine all the irreducible factors of  $X^n - \lambda$  over  $F_q$ . It is remarkable that, though all irreducible binomials over  $F_q$  have been explicitly characterized by Serret early in 1866 (e.g. see [16, Theorem 3.75] or [19, Theorem 10.7]), no effective method were found to characterize the irreducible factors of  $X^n - \lambda$  over  $F_q$  so far. It is a challenge to determine explicitly the polynomial generators of all constacyclic codes over finite fields.

It is well known that  $X^n - \lambda$  is a factor of  $X^N - 1$  for a suitable integer  $N$ , and the irreducible factors of  $X^N - 1$  over  $F_q$  with  $q = p^m$  as above can be described by the  $q$ -cyclotomic cosets. Recently, assuming that  $p$  is odd and the order of  $\lambda$  in the multiplicative group  $F_q^*$  is a power of 2, Bakshi and Raka in [2] described the polynomial generators of  $\lambda$ -constacyclic codes of length  $2^t$  over  $F_q$  by means of recognizing the  $q$ -cyclotomic cosets which are corresponding to the irreducible factors of  $X^{2^t} - \lambda$ . In the same paper [2], Bakshi and Raka determined the polynomial generators of all the  $\lambda$ -constacyclic codes of length  $2^t p^s$  over  $F_q$ ,  $q = p^m$ , for any nonzero  $\lambda$  in  $F_q$ . Almost the same time but in another approach, assuming that  $p$  is odd, Dinh in [11] determined the polynomial generators of all constacyclic codes of length  $2p^s$  over  $F_q$  in a very explicit form: the irreducible factors of the polynomial generators are all binomials of degree 1 or 2.

In this paper, we are concerned with the constacyclic codes of length  $\ell^t p^s$  over  $F_q$ , where  $q = p^m$  as before and  $\ell$  is a prime different from  $p$ . We introduce a concept “isometry” for the non-zero elements of  $F_q$  to classify constacyclic codes over  $F_q$  such that the constacyclic codes belonging to the same isometry class have the same distance structures and the same algebraic structures. Then we characterize in an explicit way the polynomial generators of constacyclic codes of length  $\ell^t p^s$  over  $F_q$  according to the isometry classes. It is notable that, except for the constacyclic codes which are isometric to cyclic codes, the irreducible factors of the polynomial generator of any constacyclic code of length  $\ell^t p^s$  over  $F_q$  are either all binomials or all trinomials.

The plan of this paper is as follows. The necessary notations and some known results to be used are provided in Section 2. In Section 3, we introduce precisely the concept of isometry, which is an equivalence relation on  $F_q^*$ ; and some necessary and sufficient conditions for any two elements of  $F_q^*$  isometric to each other are established; as a consequence, the constacyclic codes isometric to cyclic codes are described. In Section 4, we classify the constacyclic codes of length  $\ell^t p^s$  over  $F_q$  into isometry classes, characterize explicitly the polynomial generators of the constacyclic codes of each isometry class, and derive some consequences, including the main result of [11]. In Section 5, with the help of the GAP ([13]), the polynomial generators of all constacyclic codes of length 6 over  $F_{2^4}$ , all constacyclic codes of length 175 over  $F_{5^2}$  and all constacyclic codes of length 20 over  $F_{5^2}$  are computed.

## 2 Preliminaries

Throughout this paper  $F_q$  denotes a finite field with  $q$  elements where  $q = p^m$  is a power of a prime  $p$ . Let  $F_q^*$  denote the multiplicative group of  $F_q$  consisting of all non-zero elements of  $F_q$ ; and for  $\beta \in F_q^*$ , let  $\text{ord}(\beta)$  denote the order of  $\beta$  in the group  $F_q^*$ ; then  $\text{ord}(\beta)$  is a divisor of  $q - 1$ , and  $\beta$  is called a *primitive*  $\text{ord}(\beta)$ -th root of unity. It is well-known that  $F_q^*$  is a cyclic group of order  $q - 1$ , i.e.  $F_q^*$  is generated by a primitive  $(q - 1)$ -th root  $\xi$  of unity, we denote it by  $F_q^* = \langle \xi \rangle$ . For any integer  $k$ , it is known that  $\text{ord}(\xi^k) = \frac{q-1}{\gcd(k, q-1)}$ , where  $\gcd(k, q - 1)$  denotes the greatest common divisor of  $k$  and  $q - 1$ .

Assume that  $n$  is a positive integer and  $\lambda$  is a non-zero element of  $F_q$ . A linear code  $C$  of length  $n$  over  $F_q$  is said to be  $\lambda$ -constacyclic if for any code word  $(c_0, c_1, \dots, c_{n-1}) \in C$  we have that  $(\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$ . We denote by  $F_q[X]$ , the polynomial algebra over  $F_q$ , and denote by  $\langle X^n - \lambda \rangle$ , the ideal of  $F_q[X]$  generated by  $X^n - \lambda$ . Any element of the quotient algebra  $F_q[X]/\langle X^n - \lambda \rangle$  is uniquely represented by a polynomial  $a_0 + a_1X + \dots + a_{n-1}X^{n-1}$  of degree less than  $n$ , hence is identified with a word  $(a_0, a_1, \dots, a_{n-1})$  of length  $n$  over  $F_q$ ; so we have the corresponding *Hamming weight* and the *Hamming distance* on the algebra  $F_q[X]/\langle X^n - \lambda \rangle$ .

In this way, any  $\lambda$ -constacyclic code  $C$  of length  $n$  over  $F_q$  is identified with exactly one ideal of the quotient algebra  $F_q[X]/\langle X^n - \lambda \rangle$ , which is generated by a divisor  $g(X)$  of  $X^n - \lambda$ , and the divisor  $g(X)$  is determined by  $C$  uniquely up to a scale; in that case,  $g(X)$  is called a *polynomial generator* of  $C$  and write it as  $C = \langle g(X) \rangle$ . Specifically, the irreducible factorization of  $X^n - \lambda$  in  $F_q[X]$  determines all  $\lambda$ -constacyclic codes of length  $n$  over  $F_q$ .

Note that the 1-constacyclic codes are just the usual *cyclic codes*, and there is a lot of literature to deal with the cyclic codes. In particular, the irreducible factorization of  $X^n - 1$  in  $F_q[X]$  can be described as follows. As usual, we adopt the notations:  $k | n$  means that the integer  $k$  divides  $n$ ; and, for a prime integer  $\ell$ ,  $\ell^e || n$  means that  $\ell^e | n$  but  $\ell^{e+1} \nmid n$ .

**Remark 2.1.** Assume that  $n = n'p^s$  with  $s \geq 0$  and  $p \nmid n'$ . For an integer  $r$  with  $0 \leq r \leq n' - 1$ , the  $q$ -cyclotomic coset of  $r$  modulo  $n'$  is defined by

$$C_r = \{r \cdot q^j \pmod{n'} \mid j = 0, 1, \dots\}.$$

A subset  $\{r_1, r_2, \dots, r_\rho\}$  of  $\{0, 1, \dots, n' - 1\}$  is called a *complete set of representatives* of all  $q$ -cyclotomic cosets modulo  $n'$  if  $C_{r_1}, C_{r_2}, \dots, C_{r_\rho}$  are distinct and  $\bigcup_{i=1}^\rho C_{r_i} = \{0, 1, \dots, n' - 1\}$ . Take  $\eta$  to be a primitive  $n'$ -th root of unity (maybe in an extension of  $F_q$ ), and denote by  $M_\eta(X)$ , the minimal polynomial of  $\eta$  over  $F_q$ . It is well-known that (e.g. see [15, Theorem 4.1.1]):

$$X^{n'} - 1 = M_{\eta^{r_1}}(X) M_{\eta^{r_2}}(X) \cdots M_{\eta^{r_\rho}}(X) \quad (2.1)$$

with

$$M_{\eta^{r_i}}(X) = \prod_{j \in C_{r_i}} (X - \eta^j), \quad i = 1, \dots, \rho,$$

all being irreducible in  $F_q[X]$ , hence

$$X^n - 1 = (X^{n'} - 1)^{p^s} = M_{\eta^{r_1}}(X)^{p^s} M_{\eta^{r_2}}(X)^{p^s} \cdots M_{\eta^{r_\rho}}(X)^{p^s} \quad (2.2)$$

is the irreducible decomposition of  $X^n - 1$  in  $F_q[X]$ .

In a very special case the irreducible factorization of  $X^n - \lambda$  in  $F_q[X]$  has been characterized precisely, we quote it as the following remark.

**Remark 2.2.** Assume that  $q \equiv 3 \pmod{4}$  (in particular,  $q$  is a power of an odd prime), equivalently,  $2 \parallel (q-1)$ . Then  $X^{2^t} + 1$  is factorized into irreducible polynomials over  $F_q$  in [5, Theorem 1]. We should mention that, though [5, Theorem 1] is proved for a prime  $p$  with  $p \equiv 3 \pmod{4}$ , one can check in the same way as in [5] that it also holds for the present case when  $q$  is a power of a prime and  $q \equiv 3 \pmod{4}$ . We reformulate the result as follows. Note that  $4 \mid (q+1)$  in the present case, hence there is an integer  $e \geq 2$  such that  $2^e \parallel (q+1)$ . Set  $H_1 = \{0\}$ ; recursively define

$$H_i = \left\{ \pm \left( \frac{h+1}{2} \right)^{\frac{q+1}{4}} \mid h \in H_{i-1} \right\},$$

for  $i = 2, 3, \dots, e-1$ ; and set

$$H_e = \left\{ \pm \left( \frac{h-1}{2} \right)^{\frac{q+1}{4}} \mid h \in H_{e-1} \right\} = H_{e+1} = H_{e+2} = \dots.$$

Let  $t \geq 1$ . Set  $b = t$  and  $c = 0$  if  $1 \leq t \leq e-1$ ; while set  $b = e$  and  $c = 1$  if  $t \geq e$ . Then (see [5, Theorem 1] or [19, Theorem 10.13]):

$$X^{2^t} + 1 = \prod_{h \in H_t} (X^{2^{t-b+1}} - 2hX^{2^{t-b}} + (-1)^c) \quad (2.3)$$

with all the factors in the right hand side being irreducible over  $F_q$ .

Return to our general case. As we mentioned before, the irreducible non-linear binomials over  $F_q$  have been determined by Serret early in 1866 (see [16, Theorem 3.75] or [19, Theorem 10.7]), we restate it as a remark for later quotations.

**Remark 2.3.** Assume that  $n \geq 2$ . For any  $a \in F_q^*$  with  $\text{ord}(a) = k$ , the binomial  $X^n - a$  is irreducible over  $F_q$  if and only if both the following two conditions are satisfied:

- (i) Every prime divisor of  $n$  divides  $k$ , but does not divide  $(q-1)/k$ ;
- (ii) If  $4 \mid n$ , then  $4 \mid (q-1)$ .

### 3 Isometries between constacyclic codes

Let  $F_q$  be a finite field of order  $q = p^m$  and  $F_q^* = \langle \xi \rangle$  as before, where  $\xi$  is a primitive  $(q-1)$ -th root of unity. Let  $n$  be a positive integer.

Generalizing the usual equivalence between codes, we consider a kind of equivalences between the  $\lambda$ -constacyclic codes and the  $\mu$ -constacyclic codes which preserve the algebraic structures of the constacyclic codes.

**Definition 3.1.** Let  $\lambda, \mu \in F_q^*$ . We say that an  $F_q$ -algebra isomorphism

$$\varphi : F_q[X]/\langle X^n - \mu \rangle \longrightarrow F_q[X]/\langle X^n - \lambda \rangle$$

is an isometry if it preserves the Hamming distances on the algebras, i.e.

$$d_H(\varphi(\mathbf{a}), \varphi(\mathbf{a}')) = d_H(\mathbf{a}, \mathbf{a}'), \quad \forall \mathbf{a}, \mathbf{a}' \in F_q[X]/\langle X^n - \mu \rangle.$$

And, if there is an isometry between  $F_q[X]/\langle X^n - \lambda \rangle$  and  $F_q[X]/\langle X^n - \mu \rangle$ , then we say that  $\lambda$  is  $n$ -isometric to  $\mu$  in  $F_q$ , and denote it  $\lambda \cong_n \mu$ .

Obviously, the  $n$ -isometry " $\cong_n$ " is an equivalence relation on  $F_q^*$ , hence  $F_q^*$  is partitioned into  $n$ -isometry classes. If  $\lambda \cong_n \mu$ , then all the  $\lambda$ -constacyclic codes of length  $n$  are one to one corresponding to all the  $\mu$ -constacyclic codes of length  $n$  such that the corresponding constacyclic codes have the same dimension and the same distance distribution, specifically, have the same minimum distance; at that case we say that, for convenience, the  $\lambda$ -constacyclic codes of length  $n$  are *isometric* to the  $\mu$ -constacyclic codes of length  $n$ . So, it is enough to study the  $n$ -isometry classes of constacyclic codes.

**Theorem 3.2.** For any  $\lambda, \mu \in F_q^*$ , the following three statements are equivalent to each other:

- (i)  $\lambda \cong_n \mu$ .
- (ii)  $\langle \lambda, \xi^n \rangle = \langle \mu, \xi^n \rangle$ , where  $\langle \lambda, \xi^n \rangle$  denotes the subgroup of  $F_q^*$  generated by  $\lambda$  and  $\xi^n$ .
- (iii) There is a positive integer  $k < n$  with  $\gcd(k, n) = 1$  and an element  $a \in F_q^*$  such that  $a^n \lambda = \mu^k$  and the following map

$$\varphi_a : F_q[X]/\langle X^n - \mu^k \rangle \longrightarrow F_q[X]/\langle X^n - \lambda \rangle, \quad (3.1)$$

which maps any element  $f(X) + \langle X^n - \mu^k \rangle$  of  $F_q[X]/\langle X^n - \mu^k \rangle$  to the element  $f(aX) + \langle X^n - \lambda \rangle$  of  $F_q[X]/\langle X^n - \lambda \rangle$ , is an isometry.

In particular, the number of  $n$ -isometry classes of  $F_q^*$  is equal to the number of positive divisors of  $\gcd(n, q-1)$ .

*Proof.* (i)  $\Rightarrow$  (ii). By (i) we have an isometry  $\varphi$  between the algebras:

$$\varphi : F_q[X]/\langle X^n - \mu \rangle \longrightarrow F_q[X]/\langle X^n - \lambda \rangle.$$

Since  $\varphi$  preserves the Hamming distance, it must map  $X$  of weight 1 of the algebra  $F_q[X]/\langle X^n - \mu \rangle$  to an element of the algebra  $F_q[X]/\langle X^n - \lambda \rangle$  of weight 1, so there is an element  $b \in F_q^*$  and an integer  $j$  with  $0 \leq j < n$  such that

$$\varphi(X) = bX^j. \quad (3.2)$$

Consider  $\varphi(X^i) = (bX^j)^i = b^i X^{ji} \pmod{X^n - \lambda}$  for  $i = 0, 1, \dots, n-1$ ; since  $\varphi$  is a bijection, we see that any index  $e$  with  $0 \leq e \leq n-1$  must appear in the following sequence:

$$ji \pmod{n}, \quad i = 0, 1, \dots, n-1;$$

hence  $j \pmod{n}$  must be invertible, i.e.  $0 < j < n$  and  $\gcd(j, n) = 1$ . Note that  $X^n = \lambda \pmod{X^n - \lambda}$ ; further, note that  $\varphi$  is an algebra isomorphism and  $\mu \in F_q$ , we see that  $\varphi(\mu) = \mu$ , and can make the following calculation in  $F_q[X]/\langle X^n - \lambda \rangle$  (or equivalently, modulo  $X^n - \lambda$ ):

$$\mu = \varphi(\mu) = \varphi(X^n) = \varphi(X)^n = (bX^j)^n = b^n X^{jn} = b^n \lambda^j; \quad (3.3)$$

i.e. as elements of  $F_q$  we have  $\mu = \lambda^j b^n$ . Obviously,  $\langle \xi^n \rangle = \{a^n \mid a \in F_q^*\}$ . We have  $\mu \in \langle \lambda, \xi^n \rangle$ , and hence  $\langle \mu, \xi^n \rangle \subseteq \langle \lambda, \xi^n \rangle$ . On the other hand, since  $\gcd(j, n) = 1$ , there are integers  $k, h$  such that  $jk + nh = 1$ ; so

$$\mu^k = \lambda^{jk} b^{nk} = \lambda^{jk+nh} \lambda^{-nh} b^{nk} = \lambda(\lambda^{-h} b^k)^n;$$

i.e.  $\lambda = \mu^k (\lambda^{-h} b^k)^n \in \langle \mu, \xi^n \rangle$ ; and we have that  $\langle \lambda, \xi^n \rangle \subseteq \langle \mu, \xi^n \rangle$ . Thus, we get the desired conclusion:  $\langle \lambda, \xi^n \rangle = \langle \mu, \xi^n \rangle$ .

(ii)  $\Rightarrow$  (iii). Denote  $d = \gcd(n, q-1)$ . Then the subgroup  $\langle \xi^n \rangle = \langle \xi^d \rangle$ , and the quotient group

$$F_q^* / \langle \xi^n \rangle = F_q^* / \langle \xi^d \rangle = \langle \xi \rangle / \langle \xi^d \rangle$$

is a cyclic group of order  $d$ . From the statement (ii) we have that

$$\langle \lambda, \xi^n \rangle / \langle \xi^d \rangle = \langle \mu, \xi^n \rangle / \langle \xi^d \rangle;$$

which implies that, in the cyclic group  $F_q^* / \langle \xi^d \rangle$  of order  $d$ ,  $\lambda$  and  $\mu$  generate the one and the same subgroup, in particular, they have the same order in the quotient group  $F_q^* / \langle \xi^d \rangle$ . Thus there are integers  $k', h'$  such that  $\lambda = \mu^{k'} \xi^{dh'}$  and  $\gcd(k', d) = 1$ . Since  $d \mid n$ , it is known that the natural map

$$\mathbf{Z}_n^* \longrightarrow \mathbf{Z}_d^*, \quad z \pmod{n} \longmapsto z \pmod{d},$$

is a surjective homomorphism, where  $\mathbf{Z}_n^*$  denotes the multiplicative group consisting of all reduced residue classes modulo  $n$ . We can take a positive integer  $k < n$  with  $\gcd(k, n) = 1$  and  $k \equiv k' \pmod{d}$ . Then there is an integer  $h$  such that  $k' = k + dh$ . So

$$\lambda = \mu^{k'} \xi^{dh'} = \mu^{k+dh} \xi^{dh'} = \mu^k (\mu^h \xi^{h'})^d.$$

As  $(\mu^h \xi^{h'})^d \in \langle \xi^d \rangle = \langle \xi^n \rangle$ , we have an  $a \in F_q^*$  such that  $(\mu^h \xi^{h'})^d = a^{-n}$ . In a word, we have an integer  $k$  coprime to  $n$  and an  $a \in F_q^*$  such that  $a^n \lambda = \mu^k$ . Now we define an algebra homomorphism:

$$\hat{\varphi}_a : F_q[X] \longrightarrow F_q[X] / \langle X^n - \lambda \rangle,$$

by mapping  $f(X) \in F_q[X]$  to  $\hat{\varphi}_a(f(X)) = f(aX) \pmod{X^n - \lambda}$ ; since  $a$  is non-zero,  $\hat{\varphi}_a$  is obviously surjective. Noting that  $X^n = \lambda \pmod{X^n - \lambda}$ , we have

$$\hat{\varphi}_a(X^n - \mu^k) = (aX)^n - \mu^k = a^n X^n - \mu^k = a^n \lambda - \mu^k = 0 \pmod{X^n - \lambda}.$$

So the surjective algebra homomorphism  $\hat{\varphi}_a$  induces an algebra isomorphism

$$\varphi_a : F_q[X]/\langle X^n - \mu^k \rangle \longrightarrow F_q[X]/\langle X^n - \lambda \rangle,$$

which maps any element  $f(X) + \langle X^n - \mu^k \rangle$  of  $F_q[X]/\langle X^n - \mu^k \rangle$  to the element  $f(aX) + \langle X^n - \lambda \rangle$  of  $F_q[X]/\langle X^n - \lambda \rangle$ ; since  $\varphi_a$  maps any element  $X^i$  of weight 1 to an element  $a^i X^i$  of weight 1, the algebra isomorphism  $\varphi_a$  preserves Hamming distances of the algebras. we are done for the statement (iii).

(iii)  $\Rightarrow$  (i). Since the map (3.1) in the statement (iii) is an algebra isomorphism, we have that

$$0 = \varphi_a(X^n - \mu^k) = (aX)^n - \mu^k = a^n \lambda - \mu^k \pmod{X^n - \lambda};$$

that is,  $\lambda a^n = \mu^k$ . By (iii) it is assumed that  $\gcd(k, n) = 1$ , i.e. there are integers  $j, h$  such that  $kj + nh = 1$ , which also implies that  $\gcd(j, n) = 1$ ; so

$$\mu = \mu^{kj+nh} = (\mu^k)^j \mu^{nh} = (\lambda a^n)^j \mu^{hn} = \lambda^j (a^j \mu^h)^n.$$

Set  $b = a^j \mu^h$ , then  $b \in F_q^*$  and  $b^n \lambda^j = \mu$ . Since  $F_q[X]$  is a free  $F_q$ -algebra with  $X$  as a free generator, by mapping  $X$  to  $bX^j$ , we can define an algebra homomorphism:

$$\hat{\varphi} : F_q[X] \longrightarrow F_q[X]/\langle X^n - \lambda \rangle,$$

which maps any  $f(X) \in F_q[X]$  to  $\hat{\varphi}(f(X)) = f(bX^j) \pmod{X^n - \lambda}$ . Since  $j$  is coprime to  $n$ , the following

$$\hat{\varphi}(X^i) = b^i X^{ji} \pmod{X^n - \lambda}, \quad i = 0, 1, \dots, n-1,$$

form a basis of the algebra  $F_q[X]/\langle X^n - \lambda \rangle$ ; so  $\hat{\varphi}$  is a surjective algebra homomorphism. Further, we have

$$\hat{\varphi}(X^n - \mu) = (bX^j)^n - \mu = b^n X^{nj} - \mu = b^n \lambda^j - \mu = 0 \pmod{X^n - \lambda}.$$

Thus the surjective algebra homomorphism  $\hat{\varphi}$  induces an algebra isomorphism:

$$\varphi : F_q[X]/\langle X^n - \mu \rangle \longrightarrow F_q[X]/\langle X^n - \lambda \rangle,$$

which maps any element  $f(X) + \langle X^n - \mu \rangle$  of  $F_q[X]/\langle X^n - \mu \rangle$  to the element  $f(bX^j) + \langle X^n - \lambda \rangle$  of  $F_q[X]/\langle X^n - \lambda \rangle$ ; in particular,  $\varphi$  maps any element  $X^i$  of weight 1 to an element  $b^i X^{ji} \pmod{X^n - \lambda}$  of weight 1, hence  $\varphi$  preserves the Hamming distances. That is, (i) holds.

Finally, by the equivalence of (i) and (ii), the number of the  $n$ -isometry classes of  $F_q^*$  is equal to the number of the subgroups of the quotient group

$F_q^*/\langle \xi^d \rangle$  where  $d = \gcd(n, q-1)$ . The quotient  $F_q^*/\langle \xi^d \rangle$  is a cyclic group of order  $d$ , so, for any divisor  $d' \mid d$  it has a unique subgroup of order  $d'$ . Then the number of the subgroups of  $F_q^*/\langle \xi^d \rangle$  is equal to the number of the positive divisors of  $d$ . In conclusion, the number of the  $n$ -isometry classes of  $F_q^*$  is equal to the number of the positive divisors of  $\gcd(n, q-1)$ .  $\square$

**Remark 3.3.** Though the statement (i) of Theorem 3.2 states that there is an isometry  $\varphi : F_q[X]/\langle X^n - \mu \rangle \rightarrow F_q[X]/\langle X^n - \lambda \rangle$ , the statement (iii) of Theorem 3.2 exhibits a specific isometry  $\varphi_a$  such that  $\varphi_a(X) = aX$ , which outperforms  $\varphi$  in (3.2) and provides an easy way to connect the polynomial generators of the  $\lambda$ -constacyclic codes with those of the  $\mu^k$ -constacyclic codes.

In particular, taking  $\mu = 1$ , we see that  $\lambda \cong_n 1$  implies that there is an isometry  $\varphi_a : F_q[X]/\langle X^n - 1 \rangle \rightarrow F_q[X]/\langle X^n - \lambda \rangle$  such that  $\varphi(X) = aX$ . Thus for the constacyclic codes  $n$ -isometric to the cyclic codes, we have the following consequence which is closely related to [14, Lemma 3.1].

**Corollary 3.4.** *Let  $n$  be a positive integer, and  $\lambda \in F_q^*$ . The  $\lambda$ -constacyclic codes of length  $n$  are isometric to the cyclic codes of length  $n$  if and only if  $a^n \lambda = 1$  for an element  $a \in F_q^*$ ; further, in that case the map*

$$\varphi_a : F_q[X]/\langle X^n - 1 \rangle \longrightarrow F_q[X]/\langle X^n - \lambda \rangle, \quad (3.4)$$

*which maps  $f(X)$  to  $f(aX)$ , is an isometry, and*

$$X^n - \lambda = \lambda \cdot M_{\eta^{r_1}}(aX)^{p^s} M_{\eta^{r_2}}(aX)^{p^s} \cdots M_{\eta^{r_\rho}}(aX)^{p^s} \quad (3.5)$$

*is an irreducible factorization of  $X^n - \lambda$  in  $F_q[X]$ , where  $n = n'p^s$  with  $s \geq 0$  and  $p \nmid n'$ ,  $M_{\eta^i}(X)$  and  $\{r_1, \dots, r_\rho\}$  are defined in the formula (2.2); in particular, any  $\lambda$ -constacyclic code  $C$  has a polynomial generator as follows:*

$$\prod_{i=1}^{\rho} M_{\eta^{r_i}}(aX)^{e_i}, \quad 0 \leq e_i \leq p^s, \quad \forall i = 1, \dots, \rho. \quad (3.6)$$

*Proof.* By Theorem 3.2,  $\lambda \cong_n 1$  if and only if  $\langle \lambda, \xi^n \rangle = \langle 1, \xi^n \rangle = \langle \xi^n \rangle$ ; i.e.  $\lambda \cong_n 1$  if and only if  $\lambda \in \langle \xi^n \rangle$ . However,  $\langle \xi^n \rangle = \{a^n \mid a \in F_q^*\}$ ; so  $\lambda \cong_n 1$  if and only if  $\lambda = b^n$  for an element  $b \in F_q^*$ .

Assume that it is the case, i.e.  $a^n \lambda = 1$ . By the statement (iii) of Theorem 3.2, the map (3.4) is an isometry between the algebras. And, as in the formula (2.2), we have the irreducible decomposition of  $X^n - 1$  in  $F_q[X]$ :

$$X^n - 1 = M_{\eta^{r_1}}(X)^{p^s} M_{\eta^{r_2}}(X)^{p^s} \cdots M_{\eta^{r_\rho}}(X)^{p^s};$$

hence the following is an irreducible decomposition of  $(aX)^n - 1$  in  $F_q[X]$ :

$$(aX)^n - 1 = M_{\eta^{r_1}}(aX)^{p^s} M_{\eta^{r_2}}(aX)^{p^s} \cdots M_{\eta^{r_\rho}}(aX)^{p^s}.$$

However, since  $a^n = \lambda^{-1}$ , we have that  $(aX)^n = a^n X^n = \lambda^{-1} X^n$ ; thus we get the irreducible decomposition of  $X^n - \lambda$  in  $F_q[X]$  in the formula (3.5). Finally, the polynomial generator of any  $\lambda$ -constacyclic code is a divisor of  $X^n - \lambda$ , hence has the form in (3.6).  $\square$



**Corollary 3.5.** *If  $n$  is a positive integer coprime to  $q - 1$ , then there is only one  $n$ -isometry class in  $F_q^*$ ; in particular, for any  $\lambda \in F_q^*$  the  $\lambda$ -constacyclic codes of length  $n$  are isometric to the cyclic codes of length  $n$ , i.e.  $a^n \lambda = 1$  for an  $a \in F_q^*$  and all the (3.4), (3.5) and (3.6) hold.*

*Proof.* Since  $\gcd(n, q - 1) = 1$ , the conclusion is obtained immediately. It is an automorphism of the group  $F_q^*$  which maps any  $a \in F_q^*$  to  $a^n \in F_q^*$ ; thus there is a  $b \in F_q^*$  such that  $\lambda = b^n$ .  $\square$

Let  $n = n'p^s$  as in Corollary 3.4. If  $n' = 1$ , then  $n = p^s$  is coprime to  $q - 1$  and  $X^{p^s} - 1 = (X - 1)^{p^s}$ , and we get the following result at once.

**Corollary 3.6.** *For any  $\lambda \in F_q^*$  the  $\lambda$ -constacyclic codes of length  $p^s$  are isometric to the cyclic codes of length  $p^s$ ; in particular, there is an  $a \in F_q^*$  such that  $a^{p^s} \lambda = 1$  and  $X^{p^s} - \lambda = \lambda(aX - 1)^{p^s}$  is an irreducible factorization in  $F_q[X]$ ; in particular, any  $\lambda$ -constacyclic code  $C$  of length  $p^s$  has a polynomial generator  $(X - a^{-1})^i$  with  $0 \leq i \leq p^s$ .*  $\square$

**Remark 3.7.** Taking  $\lambda = -1$ , Corollary 3.6 implies that negacyclic codes of length  $p^s$  are isometric to cyclic codes of length  $p^s$ . This generalizes [10, Theorem 3.3] which showed that, in our terminology,  $\lambda$ -constacyclic codes of length  $p^s$  over  $F_{p^m}$  are isometric to the negacyclic codes of length  $p^s$  over  $F_{p^m}$ .

## 4 Constacyclic codes of length $\ell^t p^s$

Let  $F_q$  be a finite field of order  $q = p^m$  and  $F_q^* = \langle \xi \rangle$  be generated by a primitive  $(q - 1)$ -th root  $\xi$  of unity as before.

In this section, we consider constacyclic codes of length  $\ell^t p^s$  over  $F_q$ , where  $\ell$  is a prime integer different from  $p$  and  $s, t$  are non-negative integers. We will show that any  $\lambda$ -constacyclic code of length  $\ell^t p^s$  with  $\lambda \not\equiv_{\ell^t p^s} 1$  has a polynomial generator with irreducible factors all being binomials of degrees equal to powers of the prime  $\ell$  except for the case when  $\ell = 2, t \geq 2$  and  $2 \parallel (q - 1)$ ; and in the exceptional case the polynomial generator with irreducible factors all being trinomials corresponding to the factorization (2.3).

As we did in Remark 2.1, take a complete set  $\{r_1, \dots, r_\rho\}$  of representatives of  $q$ -cyclotomic cosets modulo  $\ell^t$ ; take a primitive  $\ell^t$ -th root  $\eta$  of unity (maybe in an extension of  $F_q$ ), and denote  $M_\eta(X)$  the minimal polynomial of  $\eta$  over  $F_q$ ; by the formula (2.2),

$$X^{\ell^t p^s} - 1 = (X^{\ell^t} - 1)^{p^s} = M_{\eta^{r_1}}(X)^{p^s} M_{\eta^{r_2}}(X)^{p^s} \cdots M_{\eta^{r_\rho}}(X)^{p^s} \quad (4.1)$$

is the irreducible factorization of  $X^{\ell^t p^s} - 1$  in  $F_q[X]$ . Further, assume that

$$\ell^u \parallel (q - 1), \quad \zeta = \xi^{\frac{q-1}{\ell^u}}, \quad v = \min\{t, u\}. \quad (4.2)$$

**Theorem 4.1.** *With notations as above, for any  $\lambda \in F_q^*$  there is an index  $j$  with  $0 \leq j \leq v$  such that  $\lambda \cong_{\ell^t p^s} \zeta^{\ell^j}$  and one of the following two cases holds:*

- (i)  $j = v$ , then  $\lambda \cong_{\ell^t p^s} 1$ ,  $a^{\ell^t p^s} \lambda = 1$  for an  $a \in F_q^*$  and  $X^{\ell^t p^s} - \lambda = \lambda \cdot \prod_{i=1}^p M_{\eta^{r_i}}(aX)^{p^s}$  with  $\{r_1, \dots, r_p\}$  and  $M_{\eta^{r_i}}(X)$ 's defined in (4.1).
- (ii)  $0 \leq j \leq v-1$ , then  $a^{\ell^t p^s} \lambda = \zeta^{k\ell^j}$  for an  $a \in F_q^*$  and a positive integer  $k$  coprime to  $\ell^t p^s$ ; there are two subcases:

- (ii.a) if  $\ell = 2$ ,  $t \geq 2$  and  $2 \parallel (q-1)$ , then  $j = 0$ ,  $a^{\ell^t p^s} \lambda = -1$  and, setting  $H_t$ ,  $b$  and  $c$  to be as in Remark 2.2, we have that

$$X^{2^t p^s} - \lambda = (-\lambda) \cdot \prod_{h \in H_t} (a^{2^{t-b+1}} X^{2^{t-b+1}} - 2a^{2^{t-b}} h X^{2^{t-b}} + (-1)^c)^{p^s} \quad (4.3)$$

with all the factors in the right hand side being irreducible over  $F_q$ ;

- (ii.b) otherwise, taking an integer  $s'$  with  $0 \leq s' < m$  and  $s' \equiv s \pmod{m}$ , we have that

$$X^{\ell^t p^s} - \lambda = \prod_{i=0}^{\ell^j-1} \left( X^{\ell^{t-j}} - a^{-\ell^{t-j}} \zeta^{i\ell^{u-j} + kp^{m-s'}} \right)^{p^s} \quad (4.4)$$

with all the factors in the right hand side being irreducible over  $F_q$ .

*Proof.* As  $q-1 = p^m-1$ , it is clear that  $\gcd(p^s, q-1) = 1$ . From the notation (4.2), we have

- $\zeta \in F_q$  is a primitive  $\ell^u$ -th root of unity,  $\langle \zeta \rangle$  is the Sylow  $\ell$ -subgroup of  $F_q^*$ , and  $\zeta^{\ell^{u-j}}$  for  $0 \leq j \leq u$  is a primitive  $\ell^j$ -th root of unity;
- $\ell^v = \gcd(\ell^t p^s, q-1)$ , so  $\text{ord}(\xi^{\ell^t p^s}) = \frac{q-1}{\gcd(\ell^t p^s, q-1)} = \frac{q-1}{\ell^v} = \text{ord}(\xi^{\ell^v})$ , hence in the multiplicative group  $F_q^*$  we have that

$$\langle \xi^{\ell^t p^s} \rangle = \langle \xi^{\ell^t} \rangle = \langle \xi^{\ell^v} \rangle \quad (4.5)$$

which is a subgroup of  $F_q^*$  of order  $\frac{q-1}{\ell^v}$ .

Thus the quotient group  $F_q^* / \langle \xi^{\ell^v} \rangle$  is a cyclic group of order  $\ell^v$ ; and for each positive divisor  $\ell^{v-j}$  of  $\ell^v$ , where  $j = 0, 1, \dots, v$ ,  $\langle \zeta^{\ell^j}, \xi^{\ell^v} \rangle / \langle \xi^{\ell^v} \rangle$  is the unique subgroup of order  $\ell^{v-j}$  of the quotient group  $F_q^* / \langle \xi^{\ell^v} \rangle$ .

By the equivalence (i)  $\Leftrightarrow$  (ii) of Theorem 3.2, the number of the  $\ell^t p^s$ -isometry classes of  $F_q^*$  is equal to  $v+1$ ; precisely, for any  $\lambda \in F_q^*$  there is exactly one index  $j$  with  $0 \leq j \leq v$  such that  $\lambda \cong_{\ell^t p^s} \zeta^{\ell^j}$ . We continue the discussion in two cases.

*Case (i):*  $j = v$ , i.e.  $\lambda \cong_{\ell^t p^s} \zeta^{\ell^v}$ ; by the equality (4.5), we see that  $\langle \lambda, \xi^{\ell^t p^s} \rangle = \langle \zeta^{\ell^v}, \xi^{\ell^v} \rangle = \langle 1, \xi^{\ell^t p^s} \rangle$ , in other words,  $\lambda \cong_{\ell^t p^s} 1$ . By Corollary 3.4,

$a^{\ell^t p^s} \lambda = 1^k = 1$  for an  $a \in F_q^*$ , and from the irreducible factorization (4.1) we get the irreducible factorization  $X^{\ell^t p^s} - \lambda = \lambda \cdot \prod_{i=1}^{\rho} M_{\eta^i}(aX)^{p^s}$ .

*Case (ii):*  $0 \leq j \leq v-1$ . Then by (4.2) we have

$$0 \leq j \leq v-1 < v = \min\{t, u\}, \quad (4.6)$$

in particular,  $v \geq 1$ , i.e.  $\ell \mid (q-1)$ ; further, since  $\lambda \cong_{\ell^t p^s} \zeta^{\ell^j}$ , by Theorem 3.2 (iii) there is an  $a \in F_q^*$  and a positive integer  $k$  such that

$$a^{\ell^t p^s} \lambda = \zeta^{k\ell^j}, \quad \gcd(k, \ell^t p^s) = 1. \quad (4.7)$$

We discuss it in the two subcases (ii.a) and (ii.b) as described in the theorem.

*Subcase (ii.a).* Since  $\ell = 2$ ,  $t \geq 2$  and  $2 \parallel (q-1)$ , we have that  $q$  is odd,  $t > u = v = 1$ ,  $\zeta = -1$  and  $j = 0$ ; and, from (4.7) we see that  $\ell = 2 \nmid k$  and  $a^{2^t p^s} \lambda = (-1)^k = -1$ . From the formula (2.3), we have the following irreducible factorization in  $F_q[X]$ :

$$X^{2^t p^s} + 1 = \prod_{h \in H_t} (X^{2^{t-b+1}} - 2hX^{2^{t-b}} + (-1)^c)^{p^s};$$

thus the following is an irreducible factorization of  $(aX)^{2^t p^s} + 1$  in  $F_q[X]$ :

$$(aX)^{2^t p^s} + 1 = \prod_{h \in H_t} (a^{2^{t-b+1}} X^{2^{t-b+1}} - 2a^{2^{t-b}} hX^{2^{t-b}} + (-1)^c)^{p^s}.$$

However, since  $a^{2^t p^s} = -\lambda^{-1}$ , we have that  $(aX)^{2^t p^s} = a^{2^t p^s} X^{2^t p^s} = -\lambda^{-1} X^{2^t p^s}$ ; thus we get the irreducible factorization (4.3) of  $X^{2^t p^s} - \lambda$  in  $F_q[X]$ .

*Subcase (ii.b).* Remember that the conclusion in Remark 2.3 is applied in this subcase.

By the choice of  $s'$ ,  $m - s' + s \equiv 0 \pmod{m}$ , so  $(p^m - 1) \mid (p^{m-s'+s} - 1)$ , i.e.  $p^{m-s'+s} \equiv 1 \pmod{q-1}$ ; in particular,  $\beta p^{m-s'+s} = \beta$  for any  $\beta \in F_q^*$ . Obviously,  $\zeta^{\ell^{u-j}}$  is a primitive  $\ell^j$ -th root of unity in  $F_q$ . Therefore,

$$\left( \frac{X^{\ell^{t-j}}}{\zeta^{kp^{m-s'}}} \right)^{\ell^j} - 1 = \prod_{i=0}^{\ell^j-1} \left( \frac{X^{\ell^{t-j}}}{\zeta^{kp^{m-s'}}} - \zeta^{i\ell^{u-j}} \right),$$

hence

$$\left( \frac{X^{\ell^{t-j}}}{\zeta^{kp^{m-s'}}} \right)^{\ell^j p^s} - 1 = \left( \left( \frac{X^{\ell^{t-j}}}{\zeta^{kp^{m-s'}}} \right)^{\ell^j} - 1 \right)^{p^s} = \prod_{i=0}^{\ell^j-1} \left( \frac{X^{\ell^{t-j}}}{\zeta^{kp^{m-s'}}} - \zeta^{i\ell^{u-j}} \right)^{p^s}.$$

Noting that  $\zeta^{kp^{m-s'} p^s} = (\zeta^k)^{p^{m-s'+s}} = \zeta^k$ , we get that

$$X^{\ell^t p^s} - \zeta^{k\ell^j} = \prod_{i=0}^{\ell^j-1} \left( X^{\ell^{t-j}} - \zeta^{i\ell^{u-j} + kp^{m-s'}} \right)^{p^s}. \quad (4.8)$$

From (4.7) and (4.6), we see that  $u > j$ ,  $\ell \mid (p^m - 1)$  and  $\ell \nmid k$ ; hence  $\ell \mid i\ell^{u-j}$  but  $\ell \nmid kp^{m-s'}$ . So  $\ell \nmid (i\ell^{u-j} + kp^{m-s'})$ , hence, in the multiplicative group  $F_q^*$  we have that  $\text{ord}(\zeta^{i\ell^{u-j} + kp^{m-s'}}) = \ell^u$ . By Remark 2.3, all the polynomials

$$X^{\ell^{t-j}} - \zeta^{i\ell^{u-j} + kp^{m-s'}}, \quad i = 0, 1, \dots, \ell^j - 1,$$

are irreducible polynomials in  $F_q[X]$ , and (4.8) is a irreducible factorization of  $X^{\ell^t p^s} - \zeta^{k\ell^j}$  in  $F_q[X]$ .

Replacing  $X$  by  $aX$ , we get

$$(aX)^{\ell^t p^s} - \zeta^{k\ell^j} = \prod_{i=0}^{\ell^j-1} \left( (aX)^{\ell^{t-j}} - \zeta^{i\ell^{u-j} + kp^{m-s'}} \right)^{p^s}.$$

But  $a^{\ell^t p^s} \lambda = \zeta^{k\ell^j}$ , i.e.  $a^{-\ell^t p^s} \zeta^{k\ell^j} = \lambda$ . We get the irreducible factorization of  $X^{\ell^t p^s} - \lambda$  in  $F_q[X]$  as follows:

$$X^{\ell^t p^s} - \lambda = a^{-\ell^t p^s} \prod_{i=0}^{\ell^j-1} \left( (aX)^{\ell^{t-j}} - \zeta^{i\ell^{u-j} + kp^{m-s'}} \right)^{p^s}.$$

Finally, noting that  $a^{-\ell^t p^s} = ((a^{-\ell^{t-j}})^{p^s})^{\ell^j}$ , from the above we get the desired irreducible factorization (4.4) of  $X^{\ell^t p^s} - \lambda$  in  $F_q[X]$ .  $\square$

**Remark 4.2.** With the same notation as in Theorem 4.1, we can describe the polynomial generator  $g(X)$  of any  $\lambda$ -constacyclic code  $C$  of length  $\ell^t p^s$  over  $F_q$  for the two cases as follows.

(i):  $j = v$ , then

$$g(X) = \prod_{i=1}^{\rho} M_{\eta^{r_i}}(aX)^{e_i}, \quad 0 \leq e_i \leq p^s \quad \forall i = 1, \dots, \rho.$$

By the way, we show an easy subcase of this case: if  $j = v = t$ , then  $\zeta^{\ell^{u-t}} = \xi^{\frac{q-1}{\ell^t}} \in F_q$  is a primitive  $\ell^t$ -th root of unity, hence  $X^{\ell^t} - 1 = \prod_{i=0}^{\ell^t-1} (X - \zeta^{i\ell^{u-t}})$ ; thus the polynomial generator  $g(X)$  looks simple:

$$g(X) = \prod_{i=0}^{\ell^t-1} (X - a^{-1} \zeta^{i\ell^{u-t}})^{e_i}, \quad 0 \leq e_i \leq p^s \quad \forall i = 0, \dots, \ell^t - 1. \quad (4.9)$$

(ii):  $0 \leq j < v \leq t$ , there are two subcases:

(ii.a): if  $\ell = 2$ ,  $t \geq 2$  and  $2 \parallel (q-1)$ , then

$$g(X) = \prod_{h \in H_t} (a^{2^{t-b+1}} X^{2^{t-b+1}} - 2a^{2^{t-b}} h X^{2^{t-b}} + (-1)^c)^{e_i}$$

with  $0 \leq e_i \leq p^s$  for  $i = 0, 1, \dots, 2^{b-1} - 1$ .

(ii.b): otherwise,

$$g(X) = \prod_{i=0}^{\ell^j-1} \left( X^{\ell^{t-j}} - a^{-\ell^{t-j}} \zeta^{i\ell^{u-j} + kp^{m-s'}} \right)^{e_i}$$

with  $0 \leq e_i \leq p^s$  for  $i = 0, 1, \dots, \ell^j - 1$ .

It is a special case for Theorem 4.1 that  $t = v = 1$ , i.e.  $\ell \mid (q-1)$  and  $t = 1$ ; at that case, as stated in the following corollary, there are only two  $\ell p^s$ -isometry classes in  $F_q^*$ , and any constacyclic code of length  $\ell p^s$  over  $F_q$  has a polynomial generator with all irreducible factors being binomials.

**Corollary 4.3.** *Assume that  $\ell$  is a prime such that  $\ell^u \parallel (q-1)$  with  $u \geq 1$ ,  $\zeta \in F_q$  is a primitive  $\ell^u$ -th root of unity, and  $\lambda \in F_q^*$ . Let  $C$  be a  $\lambda$ -constacyclic code of length  $\ell p^s$  over  $F_q$ . Then*

- either  $\lambda \in \langle \xi^\ell \rangle$ ,  $a^{\ell p^s} \lambda = 1$  for an  $a \in F_q$ , and we have

$$C = \left\langle \prod_{i=0}^{\ell-1} (X - a^{-1} \zeta^{i\ell^{u-1}})^{e_i} \right\rangle, \quad 0 \leq e_i \leq p^s, \quad \forall i = 0, 1, \dots, \ell-1;$$

- or  $\lambda \notin \langle \xi^\ell \rangle$ ,  $a^{\ell p^s} \lambda = \zeta^k$  for an  $a \in F_q^*$  and an integer  $k$  coprime to  $\ell p^s$ , and, taking  $s'$  such that  $0 \leq s' < m$  and  $s' \equiv s \pmod{m}$ , we have

$$C = \left\langle (X^\ell - a^{-\ell} \zeta^{kp^{m-s'}})^e \right\rangle, \quad 0 \leq e \leq p^s.$$

*Proof.* It follows from Remark 4.2 immediately. We just remark that  $\zeta^{\ell^{u-1}}$  is a primitive  $\ell$ -th root of unity, while  $\zeta^{kp^{m-s'}}$  is a primitive  $\ell^u$ -th root of unity.  $\square$

More specifically, if  $\ell = 2$  in the above corollary, we reobtain the main result of [11], as stated below in our notation.

**Corollary 4.4.** *Assume that  $2^u \parallel (q-1)$  with  $u \geq 1$ ,  $\zeta \in F_q$  is a primitive  $2^u$ -th root of unity, and  $\lambda \in F_q^*$ . Let  $C$  be a  $\lambda$ -constacyclic code of length  $2p^s$  over  $F_q$ . Then*

- either  $\lambda \in \langle \xi^2 \rangle$ ,  $a^{2p^s} \lambda = 1$  for an  $a \in F_q$ , and we have

$$C = \left\langle (X - a^{-1})^{e_0} (X + a^{-1})^{e_1} \right\rangle, \quad 0 \leq e_i \leq p^s, \quad \forall i = 0, 1;$$

- or  $\lambda \notin \langle \xi^2 \rangle$ ,  $a^{2p^s} \lambda = \zeta^k$  for an  $a \in F_q^*$  and an integer  $k$  coprime to  $2p^s$ , and, taking an integer  $s'$  such that  $0 \leq s' < m$  and  $s' \equiv s \pmod{m}$ , we have

$$C = \left\langle (X^2 - a^{-2} \zeta^{kp^{m-s'}})^e \right\rangle, \quad 0 \leq e \leq p^s.$$

*Proof.* Just note that  $\zeta^{2^{u-1}}$  is a primitive square root, i.e.  $\zeta^{2^{u-1}} = -1$ .  $\square$

## 5 Examples

By Theorem 4.1, the polynomial generators of all constacyclic codes of length  $\ell^t p^s$  over the finite field  $F_{p^m}$  are easy to be established, where  $\ell, p$  are different primes and  $s, t$  are non-negative integers. In this section, some examples are given to illustrate the result.

**Example 5.1.** Consider all constacyclic codes of length  $6 = 3 \cdot 2$  over  $F_{2^4}$ . Here,  $\ell = 3$ ,  $t = 1$ ,  $p = 2$  and  $s = 1$ . Let  $\xi$  be a primitive 15th root of unity in  $F_{2^4}$ . Since  $3 \mid (2^4 - 1)$ , it follows that there exists primitive 3rd root of unity in  $F_{2^4}$ . Therefore,  $X^3 - 1 = (X - 1)(X - \xi^5)(X - \xi^{10})$ . By Theorem 4.1, the number of the 6-isometry classes of  $F_{2^4}^*$  is 2. Hence, all the constacyclic codes are divided into two parts. The polynomial generators of all constacyclic codes are given in Table 1 and Table 2.

$\lambda$	$a$	$\lambda$ -constacyclic codes: $0 \leq j_0, j_1, j_2 \leq 2$	sizes
1	1	$\langle (X - 1)^{j_0} (X - \xi^5)^{j_1} (X - \xi^{10})^{j_2} \rangle$	$16^{6-j_0-j_1-j_2}$
$\xi^3$	$\xi^7$	$\langle (\xi^7 X - 1)^{j_0} (\xi^7 X - \xi^5)^{j_1} (\xi^7 X - \xi^{10})^{j_2} \rangle$	$16^{6-j_0-j_1-j_2}$
$\xi^6$	$\xi^4$	$\langle (\xi^4 X - 1)^{j_0} (\xi^4 X - \xi^5)^{j_1} (\xi^4 X - \xi^{10})^{j_2} \rangle$	$16^{6-j_0-j_1-j_2}$
$\xi^9$	$\xi$	$\langle (\xi X - 1)^{j_0} (\xi X - \xi^5)^{j_1} (\xi X - \xi^{10})^{j_2} \rangle$	$16^{6-j_0-j_1-j_2}$
$\xi^{12}$	$\xi^3$	$\langle (\xi^3 X - 1)^{j_0} (\xi^3 X - \xi^5)^{j_1} (\xi^3 X - \xi^{10})^{j_2} \rangle$	$16^{6-j_0-j_1-j_2}$

Table 1:  $\lambda$ -constacyclic codes of length 6 over  $F_{2^4}$ ,  $\lambda \cong_6 1$ ,  $a^6 \lambda = 1$

$\lambda$	$k$	$a$	$\lambda$ -constacyclic codes: $0 \leq j \leq 2$	sizes
$\xi$	5	$\xi^4$	$\langle (X^3 - \xi^8)^j \rangle$	$16^{6-3j}$
$\xi^4$	5	$\xi^6$	$\langle (X^3 - \xi^2)^j \rangle$	$16^{6-3j}$
$\xi^7$	5	$\xi^8$	$\langle (X^3 - \xi^{11})^j \rangle$	$16^{6-3j}$
$\xi^{10}$	5	$\xi^5$	$\langle (X^3 - \xi^5)^j \rangle$	$16^{6-3j}$
$\xi^{13}$	5	$\xi^2$	$\langle (X^3 - \xi^{14})^j \rangle$	$16^{6-3j}$
$\xi^2$	1	$\xi^3$	$\langle (X^3 - \xi)^j \rangle$	$16^{6-3j}$
$\xi^5$	1	1	$\langle (X^3 - \xi^{10})^j \rangle$	$16^{6-3j}$
$\xi^8$	1	$\xi^2$	$\langle (X^3 - \xi^4)^j \rangle$	$16^{6-3j}$
$\xi^{11}$	1	$\xi^4$	$\langle (X^3 - \xi^{13})^j \rangle$	$16^{6-3j}$
$\xi^{14}$	1	$\xi$	$\langle (X^3 - \xi^7)^j \rangle$	$16^{6-3j}$

Table 2:  $\lambda$ -constacyclic codes of length 6 over  $F_{2^4}$ ,  $\lambda \cong_6 \xi^5$ ,  $a^6 \lambda = \xi^{5k}$

**Example 5.2.** Consider all constacyclic codes of length  $175 = 7 \cdot 5^2$  over  $F_{5^2}$ . Here,  $\ell = 7$ ,  $t = 1$ ,  $p = 5$  and  $s = 2$ . Let  $\xi$  be a primitive 24th root of unity in  $F_{5^2}$ . Since  $\gcd(175, 5^2 - 1) = 1$ , by Corollary 3.5, all the constacyclic codes of length 175 are isometric to the cyclic codes of length 175. By [13], it follows that  $X^7 - 1 = (X - 1)(X^3 + \xi X^2 + \xi^{17} X - 1)(x^3 + \xi^5 X^2 + \xi^{13} X - 1)$  is the factorization

$\lambda$	$a$	$\lambda$ -constacyclic codes: $0 \leq i, j, k \leq 25$	sizes
1	1	$\langle (X-1)^i g(X)^j h(X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi$	$\xi^{17}$	$\langle (\xi^{17}X-1)^i g(\xi^{17}X)^j h(\xi^{17}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^2$	$\xi^{10}$	$\langle (\xi^{10}X-1)^i g(\xi^{10}X)^j h(\xi^{10}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^3$	$\xi^3$	$\langle (\xi^3X-1)^i g(\xi^3X)^j h(\xi^3X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^4$	$\xi^{20}$	$\langle (\xi^{20}X-1)^i g(\xi^{20}X)^j h(\xi^{20}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^5$	$\xi^{13}$	$\langle (\xi^{13}X-1)^i g(\xi^{13}X)^j h(\xi^{13}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^6$	$\xi^6$	$\langle (\xi^6X-1)^i g(\xi^6X)^j h(\xi^6X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^7$	$\xi^{23}$	$\langle (\xi^{23}X-1)^i g(\xi^{23}X)^j h(\xi^{23}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^8$	$\xi^{16}$	$\langle (\xi^{16}X-1)^i g(\xi^{16}X)^j h(\xi^{16}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^9$	$\xi^9$	$\langle (\xi^9X-1)^i g(\xi^9X)^j h(\xi^9X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{10}$	$\xi^2$	$\langle (\xi^2X-1)^i g(\xi^2X)^j h(\xi^2X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{11}$	$\xi^{19}$	$\langle (\xi^{19}X-1)^i g(\xi^{19}X)^j h(\xi^{19}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{12}$	$\xi^{12}$	$\langle (\xi^{12}X-1)^i g(\xi^{12}X)^j h(\xi^{12}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{13}$	$\xi^5$	$\langle (\xi^5X-1)^i g(\xi^5X)^j h(\xi^5X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{14}$	$\xi^{22}$	$\langle (\xi^{22}X-1)^i g(\xi^{22}X)^j h(\xi^{22}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{15}$	$\xi^{15}$	$\langle (\xi^{15}X-1)^i g(\xi^{15}X)^j h(\xi^{15}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{16}$	$\xi^8$	$\langle (\xi^8X-1)^i g(\xi^8X)^j h(\xi^8X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{17}$	$\xi$	$\langle (\xi X-1)^i g(\xi X)^j h(\xi X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{18}$	$\xi^{18}$	$\langle (\xi^{18}X-1)^i g(\xi^{18}X)^j h(\xi^{18}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{19}$	$\xi^{11}$	$\langle (\xi^{11}X-1)^i g(\xi^{11}X)^j h(\xi^{11}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{20}$	$\xi^4$	$\langle (\xi^4X-1)^i g(\xi^4X)^j h(\xi^4X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{21}$	$\xi^{21}$	$\langle (\xi^{21}X-1)^i g(\xi^{21}X)^j h(\xi^{21}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{22}$	$\xi^{14}$	$\langle (\xi^{14}X-1)^i g(\xi^{14}X)^j h(\xi^{14}X)^k \rangle$	$25^{175-i-3j-3k}$
$\xi^{23}$	$\xi^7$	$\langle (\xi^7X-1)^i g(\xi^7X)^j h(\xi^7X)^k \rangle$	$25^{175-i-3j-3k}$

Table 3:  $\lambda$ -constacyclic codes of length 175 over  $F_{5^2}$ ,  $\lambda \cong_{175} 1$ ,  $a^{175}\lambda = 1$

of  $X^7 - 1$  into irreducible factors over  $F_{5^2}$ . Let  $g(X) = X^3 + \xi X^2 + \xi^{17}X - 1$  and  $h(X) = x^3 + \xi^5 X^2 + \xi^{13}X - 1$ . The polynomial generators of constacyclic codes are given in Table 3.

**Example 5.3.** Consider all constacyclic codes of length  $20 = 2^2 \cdot 5$  over  $F_{5^2}$ . Here,  $\ell = 2$ ,  $t = 2$ ,  $p = 5$  and  $s = 1$ . Let  $\xi$  be a primitive 24th root of unity in  $F_{5^2}$ . Since  $4 \mid (5^2 - 1)$ , it follows that there exists a primitive 4th root of identity in  $F_{5^2}$ . Therefore,  $X^4 - 1 = (X - 1)(X - \xi^6)(X - \xi^{12})(X - \xi^{18})$ . By Theorem 4.1, the number of the 20-isometry classes of  $F_{2^4}^*$  is 3. The polynomial generators of constacyclic codes are given in Table 4-6.

$\lambda$	$a$	$\lambda$ -constacyclic codes: $0 \leq j_0, j_1, j_2, j_3 \leq 5$	sizes
1	$\xi^6$	$\langle (\xi^6 X - 1)^{j_0} (\xi^6 X - \xi^6)^{j_1} (\xi^6 X - \xi^{12})^{j_2} (\xi^6 X - \xi^{18})^{j_3} \rangle$	$25^{20-j_0-j_1-j_2-j_3}$
$\xi^4$	$\xi$	$\langle (\xi X - 1)^{j_0} (\xi X - \xi^6)^{j_1} (\xi X - \xi^{12})^{j_2} (\xi X - \xi^{18})^{j_3} \rangle$	$25^{20-j_0-j_1-j_2-j_3}$
$\xi^8$	$\xi^2$	$\langle (\xi^2 X - 1)^{j_0} (\xi^2 X - \xi^6)^{j_1} (\xi^2 X - \xi^{12})^{j_2} (\xi^2 X - \xi^{18})^{j_3} \rangle$	$25^{20-j_0-j_1-j_2-j_3}$
$\xi^{12}$	$\xi^3$	$\langle (\xi^3 X - 1)^{j_0} (\xi^3 X - \xi^6)^{j_1} (\xi^3 X - \xi^{12})^{j_2} (\xi^3 X - \xi^{18})^{j_3} \rangle$	$25^{20-j_0-j_1-j_2-j_3}$
$\xi^{16}$	$\xi^4$	$\langle (\xi^4 X - 1)^{j_0} (\xi^4 X - \xi^6)^{j_1} (\xi^4 X - \xi^{12})^{j_2} (\xi^4 X - \xi^{18})^{j_3} \rangle$	$25^{20-j_0-j_1-j_2-j_3}$
$\xi^{20}$	$\xi^5$	$\langle (\xi^5 X - 1)^{j_0} (\xi^5 X - \xi^6)^{j_1} (\xi^5 X - \xi^{12})^{j_2} (\xi^5 X - \xi^{18})^{j_3} \rangle$	$25^{20-j_0-j_1-j_2-j_3}$

Table 4:  $\lambda$ -constacyclic codes of length 20 over  $F_{5^2}$ ,  $\lambda \cong_{20} 1$ ,  $a^{20}\lambda = 1$

$\lambda$	$k$	$a$	$\lambda$ -constacyclic codes: $0 \leq j \leq 5$	sizes
$\xi$	3	$\xi^4$	$\langle (X^4 - \xi^5)^j \rangle$	$25^{20-4j}$
$\xi^5$	3	$\xi^{23}$	$\langle (X^4 - \xi^5)^j \rangle$	$25^{20-4j}$
$\xi^9$	3	$\xi^6$	$\langle (X^4 - \xi^{21})^j \rangle$	$25^{20-4j}$
$\xi^{13}$	3	$\xi$	$\langle (X^4 - \xi^{14})^j \rangle$	$25^{20-4j}$
$\xi^{17}$	3	$\xi^2$	$\langle (X^4 - \xi^{13})^j \rangle$	$25^{20-4j}$
$\xi^{21}$	3	$\xi^3$	$\langle (X^4 - \xi^9)^j \rangle$	$25^{20-4j}$
$\xi^3$	1	1	$\langle (X^4 - \xi^{15})^j \rangle$	$25^{20-4j}$
$\xi^7$	1	$\xi$	$\langle (X^4 - \xi^{11})^j \rangle$	$25^{20-4j}$
$\xi^{11}$	1	$\xi^2$	$\langle (X^4 - \xi^7)^j \rangle$	$25^{20-4j}$
$\xi^{15}$	1	$\xi^3$	$\langle (X^4 - \xi^3)^j \rangle$	$25^{20-4j}$
$\xi^{19}$	1	$\xi^4$	$\langle (X^4 - \xi^{23})^j \rangle$	$25^{20-4j}$
$\xi^{23}$	1	$\xi^5$	$\langle (X^4 - \xi^{19})^j \rangle$	$25^{20-4j}$

Table 5:  $\lambda$ -constacyclic codes of length 20 over  $F_{5^2}$ ,  $\lambda \cong_{20} \xi^3$ ,  $a^{20}\lambda = \xi^{3k}$

$\lambda$	$k$	$a$	$\lambda$ -constacyclic codes: $0 \leq j_0, j_1 \leq 5$	sizes
$\xi^2$	1	$\xi^{23}$	$\langle (X^2 - \xi^5)^{j_0} (X^2 + \xi^5)^{j_1} \rangle$	$25^{20-2j_0-2j_1}$
$\xi^6$	1	$\xi^6$	$\langle (X^2 - \xi^{15})^{j_0} (X^2 + \xi^{15})^{j_1} \rangle$	$25^{20-2j_0-2j_1}$
$\xi^{10}$	1	$\xi$	$\langle (X^2 - \xi)^{j_0} (X^2 + \xi)^{j_1} \rangle$	$25^{20-2j_0-2j_1}$
$\xi^{14}$	1	$\xi^2$	$\langle (X^2 - \xi^{23})^{j_0} (X^2 + \xi^{23})^{j_1} \rangle$	$25^{20-2j_0-2j_1}$
$\xi^{18}$	1	$\xi^3$	$\langle (X^2 - \xi^{18})^{j_0} (X^2 + \xi^{18})^{j_1} \rangle$	$25^{20-2j_0-2j_1}$
$\xi^{22}$	1	$\xi^4$	$\langle (X^2 - \xi^{11})^{j_0} (X^2 + \xi^{11})^{j_1} \rangle$	$25^{20-2j_0-2j_1}$

Table 6:  $\lambda$ -constacyclic codes of length 20 over  $F_{5^2}$ ,  $\lambda \cong_{20} \xi^6$ ,  $a^{20}\lambda = \xi^{6k}$

## Acknowledgements

This work was supported by NSFC, Grant No. 11171370, and Research Funds of CCNU, Grant No. 11A02014. The authors would like to thank the anonymous referees for their many helpful comments.



## References

- [1] T. Abualrub, R. Oehmke, On the generators of  $\mathbf{Z}_4$  cyclic codes of length  $2^e$ , *IEEE Trans. Inform. Theory*, **49**(9)(2003), 2126-2133.
- [2] G. K. Bakshi, M. Raka, A class of constacyclic codes over a finite field, *Finite Fields Appl.*, **18**(2012), 362-377.
- [3] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill Book Company, New York, 1968.
- [4] T. Blackford, Negacyclic codes over  $\mathbf{Z}_4$  of even length, *IEEE Trans. Inform. Theory*, **49**(6)(2003), 1417-1424.
- [5] I. F. Blake, S. Gao, R. C. Mullin, Explicit factorization of  $X^{2^k} + 1$  over  $F_p$  with prime  $p \equiv 3 \pmod{4}$ , *Appl. Algebra Engrg. Comm. Comput.*, **4**(1993), 89-94.
- [6] G. Castagnoli, J. L. Massey, P. A. Schoeller, N. von Seemann, On repeated-root cyclic codes, *IEEE Trans. Inform. Theory*, **37**(8)(1991), 337-342.
- [7] H. Q. Dinh, S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory*, **50**(8)(2004), 1728-1744.
- [8] H. Q. Dinh, Negacyclic codes of length  $2^s$  over Galois rings, *IEEE Trans. Inform. Theory*, **51**(12)(2005), 4252-4262.
- [9] H. Q. Dinh, On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions, *Finite Fields Appl.*, **14**(2008), 22-40.
- [10] H. Q. Dinh, Constacyclic codes of length  $p^s$  over  $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ , *Journal of Algebra*, **324** (2010), 940-950.
- [11] H. Q. Dinh, Repeated-root constacyclic codes of length  $2p^s$ , *Finite Fields Appl.*, **18**(2012), 133-143.
- [12] S. T. Dougherty, S. Ling, Cyclic codes over  $\mathbf{Z}_4$  of even length, *Designs Codes Cryptogr.*, **39**(2), (2006), 127-153.
- [13] [GAP] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.12; (<http://www.gap-system.org>), 2008.
- [14] G. Hughes, Constacyclic codes, cocycles and a  $u + v|u - v$  construction, *IEEE Trans. Inform. Theory*, **46**(2)(2000), 674-680.
- [15] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
- [16] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 2008.

- [17] A. Sălăgean, Repeated-root cyclic and negacyclic codes over a finite chain ring, *Discrete Math. Appl.*, **154**(2006), 413-419.
- [18] J. H. van Lint, Repeated-root cyclic codes, *IEEE Trans. Inform. Theory*, **37**(2)(1991), 343-345.
- [19] Z. X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing, 2003.
- [20] J. Wolfmann, Negacyclic and cyclic codes over  $Z_4$ , *IEEE Trans. Inform. Theory*, **45**(7)(1999), 2527-2532.
- [21] S. Zhu, X. Kai, A class of constacyclic codes over  $\mathbf{Z}_{p^m}$ , *Finite Fields Appl.*, **16**(2010), 243-254.